



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/936,834	03/12/2002	Thomas Breitbach	P-44 MG	1508
7590	03/23/2006		EXAMINER	LU, ZHIYU
Lackenbach Siegel One Chase Road Scarsdale, NY 10583			ART UNIT	PAPER NUMBER
			2618	

DATE MAILED: 03/23/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/936,834	BREITBACH ET AL.	
	Examiner Zhiyu Lu	Art Unit 2618	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) Responsive to communication(s) filed on 12 March 2002.

2a) This action is **FINAL**. 2b) This action is non-final.

3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) Claim(s) 1,2 and 20-36 is/are pending in the application.
4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) Claim(s) _____ is/are allowed.

6) Claim(s) 1,2 and 20-36 is/are rejected.

7) Claim(s) _____ is/are objected to.

8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) The specification is objected to by the Examiner.

10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.

 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a) All b) Some * c) None of:

1. Certified copies of the priority documents have been received.
2. Certified copies of the priority documents have been received in Application No. _____.
3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) Notice of References Cited (PTO-892)
2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____
4) Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
5) Notice of Informal Patent Application (PTO-152)
6) Other: _____

DETAILED ACTION

Claim Objections

1. Claims 1-2 and 20-36 are objected to because of the following informalities:

In line 1 of claim 1, replace “Method for” with “A method for” to denote single.

In line 1 of claims 2 and 20-36, replace “Method as” with “The method as” to denote antecedent basis.

Appropriate correction is required.

Drawings

2. The drawings are objected to because Fig. 2 shows a plurality of text blocks without step/process priority indication. Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as “amended.” If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for consistency. Additional replacement sheets may be necessary to show the renumbering of the remaining figures. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either “Replacement Sheet” or “New Sheet” pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner,

the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claims 1-2, 21-34, and 36 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 1 recites the limitation "the HBCI transmission method" in lines 2-3. There is insufficient antecedent basis for this limitation in the claim.

Claim 2 recites the limitation "the SIM card" in line 2. There is insufficient antecedent basis for this limitation in the claim.

Claim 21 recites the limitation "the HBCI protocol", "the GSM SIM card", and "the SIM card" in lines 1-2 and 4. There is insufficient antecedent basis for this limitation in the claim.

Claim 22 recites the limitation "the information exchange" in lines 1-2 and "the Short Message Service" in line 3. There is insufficient antecedent basis for this limitation in the claim.

Claim 23 recites the limitation "both subroutes" in line 1. There is insufficient antecedent basis for this limitation in the claim.

Claim 24 recites the limitation "the security protocol" and "SIM card" in line 2. There is insufficient antecedent basis for this limitation in the claim.

Claim 25 recites the limitation "the second security protocol" in line 1. There is insufficient antecedent basis for this limitation in the claim.

Claim 26 recites the limitation "the SIM card", "the second security protocol", and "the regular SIM card personalization" in lines 2-3. There is insufficient antecedent basis for this limitation in the claim.

Claim 27 recites the limitation "the key", "the subscriber", "the SM card", and "the mobile telephone" in lines 1-3. There is insufficient antecedent basis for this limitation in the claim.

Claim 28 recites the limitation "the subscriber", "the PIN" and "the key" in lines 1-2. There is insufficient antecedent basis for this limitation in the claim.

Claim 29 recites the limitation "the card personalization", "the mobile telephone network operator", "the bank application", "the Ksms", and "all SIM cards" in lines 1-3. There is insufficient antecedent basis for this limitation in the claim.

Claim 30 recites the limitation "the service", "the subscriber", and "the data" in lines 1-2. There is insufficient antecedent basis for this limitation in the claim.

Claim 31 recites the limitation "the initialization", "the application", "the KIV", "the initialization PIN", "the key", "the local PIN", "the bank routing number", and "the account number" in lines 1-4. There is insufficient antecedent basis for this limitation in the claim.

Claim 32 recites the limitation "the generation", "the Ksms", "the initialization PIN", and "the gateway operator" in lines 1-2. There is insufficient antecedent basis for this limitation in the claim.

Claim 33 recites the limitation "the generation", "the initialization PIN", and "the bank" in line 2. There is insufficient antecedent basis for this limitation in the claim.

Claim 34 recites the limitation "the authentication" and "the initialization PIN" in lines 1-3.

There is insufficient antecedent basis for this limitation in the claim.

Claim 36 recites the limitation "the subscriber", "the identification", and "the calling line identification" in lines 1-3. There is insufficient antecedent basis for this limitation in the claim.

Claim 28 recites, "... the subscriber is informed per PIN letter by the bank of the PIN for generating the key (Ksms)", which is unable to clarify the subject matter disclosed in the filed specification. Corresponding to the 3rd paragraph in page 5, the Examiner takes the claim interruption as the subscriber is informed a PIN in a letter for generating the key (Ksms) by the bank.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. Claims 1-23 and 36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hultgren (US Patent#6868391).

Regarding claim 1, Hultgren teaches method for using standardized bank services via mobile radiotelephone, wherein the data transmission between a bank server and a mobile station builds on the transmission method, characterized in that an gateway (30 of Fig. 1) is inserted into the

transmission path between the bank server (80 of Fig. 1) and the mobile station (60 of Fig. 1), which carries out a transformation between the transmission method used at the bank end and a transmission method used at the mobile radiotelephone end (Fig. 1, column 3 line 39 to column 4 line 47).

Hultgren does not expressly disclose the limitation of using HBCI data transmission implementation.

However, HBCI is a common standardized bank software system used in European market. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate HBCI data transmission implementation into the method of Hultgren, in order to gain on popularity, compatibility, and support.

Regarding claim 2, Hultgren teaches the limitation of claim 1.

Hultgren also teaches the limitation of characterized in that a splitting of the customer-end HBCI system into two components, the SIM card of the mobile station and the HBCI gateway takes place (column 12 line 59 to column 13 line 21).

Regarding claim 20, Hultgren teaches the limitation of claim 1.

Hultgren also teaches the limitation of characterized in that two transmission routes are formed, firstly between SIM card and HBCI gateway (between 60 and 30 of Fig. 1) and secondly between HBCI gateway and bank server (between 30 and 80 of Fig. 1) (column 12 line 59 to column 13 line 21).

Regarding claim 21, Hultgren teaches the limitation of claim 1.

Hultgren also teaches the limitation of the HBCI protocol is unpacked by the HBCI gateway and its protocol sequence is converted such that compatibility with the GSM SIM card and the GSM network is obtained in order for an exchange of the converted protocol with the SIM card is to be possible (column 13 lines 22-32).

Regarding claim 22, Hultgren teaches the limitation of claim 1.

Hultgren also teaches the limitation of a carrier service for the information exchange between HBCI gateway and mobile station serves a GSM data transmission service, in particular the Short Message Service (column 13 lines 22-32).

Regarding claim 23, Hultgren teaches the limitation of claim 1.

Hultgren also teaches the limitation of on both subroutines a cryptographic security is realized (column 6 lines 38-43, column 12 lines 59-65).

Regarding claim 36, Hultgren teaches the limitation of claim 1.

Hultgren also teaches the limitation of an additional authentication of the subscriber takes place via the identification of his mobile connection thereby that an evaluation of the calling line identification (CLI) is carried out (column 13 lines 33-49).

5. Claims 24-28, 30-31 and 34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hultgren (US Patent#6868391) in view of HBCI Interface Specification (http://www.hbci-zka.de/english/documents/specification_english/Coll_HBCI21e.pdf).

Regarding claim 24, Hultgren teaches the limitation of claim 1.

But, Hultgren does not expressly disclose the limitation of between bank server and HBCI gateway the security protocol defined by HBCI is applied and between HBCI gateway and SIM card a second security protocol is employed.

HBCI Interface Specification teaches the limitation of between bank server and HBCI gateway the security protocol defined by HBCI is applied and between HBCI gateway and SIM card a second security protocol is employed (III.1.3), where the first security protocol between HBCI gateway and SIM card is the regular security protocol with the SIM card itself.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate security protocol of HBCI in transmission routes taught by HBCI Interface Specification into the method of Hultgren, in order to enhance information security protection.

Regarding claim 25, Hultgren teaches the limitation of claim 1.

But, Hultgren does not expressly disclose the limitation of the second security protocol corresponds to a protocol reduced in terms of data quality but equivalent to HBCI in terms of security technology.

HBCI Interface Specification teaches the limitation of the second security protocol corresponds to a protocol reduced in terms of data quality but equivalent to HBCI in terms of security

technology (III.1.3), where customer chooses the encryption algorithm to be used, wherein the encryption algorithm is supported by the bank and fit for security procedure and compression procedure of HBCI.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate security protocol with reduced data size and equivalent HBCI security taught by HBCI Interface Specification into the method of Hultgren, in order to enhance information security protection and reduce traffic load.

Regarding claim 26, Hultgren teaches the limitation of claim 1.

But, Hultgren does not expressly disclose the limitation of a cryptographic key (Ksms) specific to each subscriber is securely generated and stored in the SIM card for use in the second security protocol after the regular SIM card personalization.

HBCI Interface Specification teaches the limitation of a cryptographic key (Ksms) (signature key) specific to each subscriber is securely generated and stored in the SIM card (Chip card of Fig. 1) for use in the second security protocol (I Introduction, VI.3.1.1 Key types) after the regular SIM card personalization.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate generating cryptographic key to each subscriber taught by HBCI Interface Specification into the method of Hultgren, in order to authenticate and secure transaction.

Regarding claim 27, Hultgren teaches the limitation of claim 1.

But, Hultgren does not expressly disclose the limitation of the generation of the key (Ksms) specific to the subscriber is generated in the SIM card by entering an initialization PIN on the mobile telephone.

HBCI Interface Specification teaches the limitation of the generation of the key (Ksms) specific to the subscriber is generated in the SIM card by entering an initialization PIN (User ID) on the mobile telephone (VI.3.1.1 Key names).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate generating key with entering initialization PIN taught by HBCI Interface Specification into the method of Hultgren, in order to generate a reliable concrete key instead of random generation.

Regarding claim 28, Hultgren teaches the limitation of claim 1.

But, Hultgren does not expressly disclose the limitation of the subscriber is informed per PIN letter by the bank of the PIN for generating the key (Ksms) (VI.3.1.3.2 Initial key distribution, in writing from the bank).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate informing subscriber PIN number in letter by the bank taught by HBCI Interface Specification into the method of Hultgren, in order to inform subscriber security generating PIN in a more securable way.

Regarding claim 30, Hultgren teaches the limitation of claim 1.

But, Hultgren does not expressly disclose the limitation of before subscription to the service the subscriber receives the data of his bank including an initialization PIN.

HBCI Interface Specification teaches the limitation of before subscription to the service the subscriber receives the data of his bank including an initialization PIN (User ID of III.1.1, VI.3.1.3.2 Initial key distribution)

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate providing user an initialization PIN from his bank taught by HBCI Interface Specification into the method of Hultgren, in order to enable user to use service with security.

Regarding claim 31, Hultgren teaches the limitation of claim 1.

But, Hultgren does not expressly disclose the limitation of during the initialization of the application, i.e. during subscription, with the aid of the KIV from initialization PIN, the key Ksms is generated through triple DES using the local PIN, the bank routing number and the account number.

HBCI Interface Specification teaches a cryptographic method of generating the key through triple DES using country code (local PIN), bank code (routing number), user ID (account number), key type, key number, and version number (VI.3.1.1, II.5.3.2).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate generating key through triple DES using local PIN, bank routing number, and account number taught by HBCI Interface Specification into the method of Hultgren, in order to have verifiable key generating components.

Regarding claim 34, Hultgren teaches the limitation of claim 1.

But, Hultgren does not expressly disclose the limitation of the authentication of the two involved sites, mobile radiotelephone subscriber and HBCI gateway, takes place by knowledge of the initialization PIN exchanged in writing.

HBCI Interface Specification teaches the limitation of the authentication of the two involved sites, mobile radiotelephone subscriber and HBCI gateway, takes place by knowledge of the initialization PIN exchanged in writing (VI.3.1.3.2).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the initialization PIN exchange in writing into the method of Hultgren, in order to provide official and authentic PIN exchange.

6. Claim 32 is rejected under 35 U.S.C. 103(a) as being unpatentable over Hultgren (US Patent#6868391) in view of Fujioka (JP10-242957).

Regarding claim 32, Hultgren teaches the limitation of claim 1.

But, Hultgren does not expressly disclose the limitation of for the generation of the Ksms in the HBCI gateway the initialization PIN is transferred to the gateway operator.

Fujioka teaches the limitation of transferring a initial key to server for generating another key (abstract).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate transferring initialization PIN to server for generating a key taught by Fujioka into the method of Hultgren, in order to authenticate key generation for the right client.

7. Claims 29 and 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hultgren (US Patent#6868391) in view of Atalla (US Patent#4288659).

Regarding claim 29, Hultgren teaches the limitation of claim 1.

But, Hultgren does not expressly disclose the limitation of during the card personalization by the mobile telephone network operator together with the bank application, an initialization key KIV, derived from a master key and a SIM card-individual number, for generating the Ksms specific to the subscriber is applied onto all SIM cards.

Atalla teaches the limitation of generating an initialization key based on a secret code (master key) known by both authorized individual and the bank and an identification of the terminal for generating the session key specific to the terminal user (column 1 line 45 to column 2 line 27).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate generating initialization key from a master key and a hardware individual number taught by Atalla into the method of Hultgren, in order to provide both user and hardware authentication in initialization.

Regarding claim 33, Hultgren teaches the limitation of claim 1.

But, Hultgren does not expressly disclose the limitation of the generation of the initialization PIN takes place at the HBCI gateway and this is transferred to the bank.

Atalla teaches the limitation of the generation of the initialization PIN takes place at the terminal (mid-node between user and bank) and data terminal must be initialized in the first operating cycle (column 1 line 45 to column 2 line 27, column 2 lines 64-67).

Considering the connection between the user and the bank, it would have been obvious to one of ordinary skill in the art to recognize that the gateway is the mid-node authentication process for the user to proceed first before getting to the bank. The gateway would be the one who masters connections with the user and the bank. The gateway would be the first node to authenticate user and to initialize session. Thus, it would have been obvious to one of ordinary skill in the art to recognize that it is convenient and secure for the gateway to generate initialization PIN and then transfer it to the bank so that the bank can inform user the initialization key since the bank is the one who authorize the service.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate generating initialization key in mid-node taught by Atalla into the method of Hultgren and modify into transferring the generated initialization key to the bank, in order to provide secured user initialization and authentication in the HBCI gateway.

8. Claim 35 is rejected under 35 U.S.C. 103(a) as being unpatentable over Hultgren (US Patent#6868391) in view of Elgamal et al. (US Patent#5657390).

Regarding claim 35, Hultgren teaches the limitation of claim 1.

But, Hultgren does not expressly disclose the limitation of between mobile radiotelephone network operator and HBCI gateway operator a master key is exchanged.

Elgamal et al. teach the limitation of between mobile radiotelephone network operator and HBCI gateway operator a master key is exchanged (column 7 lines 41-56).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate exchanging master key taught by Elgamal et al. into the method of Hultgren, in order for both client and server to produce session keys that would be employed to actually encrypt/decrypt data.

Conclusion

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zhiyu Lu whose telephone number is (571) 272-2837. The examiner can normally be reached on Weekdays: 9AM-5PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nay Maung can be reached on (571)272-7882. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Zhiyu Lu
March 13, 2006


NAY MAUNG
SUPERVISORY PATENT EXAMINER